china's golden shield

Corporations and the Development of Surveillance Technology in the People's Republic of China

enter

by
Greg Walton

Rights & Democracy is a Canadian institution with an international mandate. It works with civil society and governments in Canada and abroad to promote human rights and democratic development through dialogue, advocacy, capacity building and public education. It focuses on four themes: democratic development, women's rights, rights of indigenous peoples, and globalization and human rights; as well as two special operations: International Human Rights Advocacy and Urgent Action/Important Opportunities.

Author:
Greg Walton is a freelance researcher focusing on the impact of technology and globalization on human rights and democracy. He is currently developing disruptive compliance strategies for a range of transnational, non-profit organizations. His homepage is go.openflows.org/jamyang.

Acknowledgements:
Carole Samdup, Diana Bronson, and all at Team R&D. OxBlood Ruffin, cDc, Drunken Master and the Hacktivismo! Project. y Oda, the Google cache, Kundrel core, SafeWeb, Dr. Patrick Ball, Jenny 8, Wyrds of Simple Nomad, Openflows, M&D, and so many others – on both sides of the firewall – who very sensibly choose to remain anonymous. For now ;-)

© International Centre for Human Rights and Democratic Development, 2001.

This publication is available free of charge and may be freely excerpted, provided credit is given and a copy of the publication in which the material appears is sent to Rights & Democracy.

Legal Deposit: Bibliothèque nationale du Québec, fourth quarter 2001.
National Library of Canada, fourth quarter 2001. ISBN: 2-922084-42-6.

Graphics: Laperrière Communication
Printed in Canada.

China's Golden Shield 1.0 is available at www.ichrdd.ca.
It is also published as an Open Source Human Rights Report at: go.openflows.org.

FREEDOM_OF_SPEECH : FREEDOM_OF_CODE

China's Golden Shield

Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.

The Universal Declaration of Human Rights, Article 28

"... it's a little strange to tie free trade to human rights issues, it is basically getting down to interference in internal affairs."[1]

Bill Gates, then CEO of Microsoft,
standing shoulder to shoulder with Jiang Zemin during a photo-op in Beijing, 1994.

Table of Contents

Preface 04
Executive Summary 05
Introduction 08
Box 1: Paying the Price for Freedom 10

Technology Transfer and Policy Convergence 11
Operation Root Canal 12

What do You Want the Internet to Be?
"A human touch. I want it to know who I am." 14
China's Golden Shield 15
Box 2: China's Golden Projects: Modernizing the Chinese Economy 17
Unholy Alliance 17
Beyond the Great Firewall 18
Making the Internet Personal 20
The Subscriber Edge 23
A Virtual Shadow 24
A Network that Knows Who and Where You Are 25
Box 3: "Neutral" Technology at Tiananmen Square 26
Diagram 1: A New Model for the Internet: Innovation at the Edge of the Network 27
Diagram 2: Interaction Across a Firewall 27

Conclusion – "The mouse is mightier than the missile" 28
Appendix: How to Use the CD-ROM that Accompanies this Report 29
Liner Notes 30

Glossary 32

Endnotes 36

Preface

Information and communication technology is often described as the driving force behind globalization. It is also promoted as a tool for democratization with connectivity heralded as the end of the digital divide. In truth, there is no doubt that electronic communication has facilitated the flow of information around the globe and that it has increased opportunities for human rights and democracy activists to build international support for their struggles.

Unfortunately, the advent of modern communication technology has also brought new challenges for human rights advocates, particularly those living under repressive regimes. In a world where the rules of international trade are unconnected to international human rights law, technology's promise of democratization is threatened by economic priorities. In the People's Republic of China, where there is no democratic accountability or legislative protection of human rights, technology can be and has been used as an instrument of repression.

At stake is the right of all people to an international order within which the promise of the Universal Declaration of Human Rights (UDHR) can be fulfilled. The UDHR and its accompanying covenant on civil and political rights protect fundamental human rights including the individual's right to privacy. The protection of human rights is the obligation of governments and must be reflected in all activities implemented under governmental authority whether they are trade promotion activities, the negotiation of bilateral and international trade agreements, export financing or development assistance.

This report reveals how sophisticated technology, developed in Canada and promoted through a series of national and international processes, could undermine the principles enshrined in human rights agreements. China's Golden Shield project threatens the protection of human rights, in particular the right to privacy – a right that underpins other essential elements of democracy activism such as freedom of association and freedom of expression. It positions the alliance of government and business in opposition to those standing on the cyber-frontline of the human rights movement in China today.

It is my hope that this paper will provide a glimpse into the world of high-tech, big business and the struggle for human rights and democracy in China. On behalf of Rights & Democracy, I offer it in the spirit of solidarity with the people of China who may find its content of some use as they develop and consolidate social movements for change. I offer it also to my fellow Canadians who, following recent reports on police surveillance of dissent in Canada, may discover how intimately the rights of citizens in China are linked to our own.

Warren Allmand, P.C., O.C., Q.C.

President

Executive Summary

China today faces a very modern paradox. On one side, the government understands that information technologies are the engine driving the global economy, and that Chinese economic growth will depend in large measure on the extent to which the country is integrated with the global information infrastructure. At the same time, however, China is an authoritarian, single-party state. Continued social stability relies on the suppression of anti-government activities. To state the problem simply, political control is dependent on economic growth and economic growth requires the modernization of information technologies, which in turn, have the potential to undermine political control.

The "Great Firewall of China" is failing, largely due to the increased volume of Internet traffic in China. The government knows that it can no longer hope to filter out all "objectionable" material before it enters China's networks; and so, faced with these contradictory forces of openness and control, China is seeking to strike a balance between the information-related needs of economic modernization and the security requirements of internal stability. In seeking to reach this balance, the Chinese state has found an extraordinary ally in private telecommunications firms located primarily in Western countries. Many companies, including notably Nortel Networks, until recently Canada's largest firm, are playing key roles in meeting the security needs of the Chinese government. Nortel Networks and other international firms are in effect helping China to displace the firewall it constructed at the international gateway with a more sophisticated system of content filtration at the individual level.

Old style censorship is being replaced with a massive, ubiquitous architecture of surveillance: the Golden Shield. Ultimately the aim is to integrate a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies. This has been facilitated by the standardization of telecommunications equipment to facilitate electronic surveillance, an ambitious project led by the Federal Bureau of Investigation (FBI) in the US, and now adopted as an international standard.

Many people in China have been arrested for Internet-related "crimes," ranging from supplying e-mail addresses to Internet publications to circulating pro-democratic information or articles that are critical of the Chinese government, in blatant contradiction of international human rights law guaranteeing freedom of speech. Charges are typically "subversion" or "threatening to overthrow the government" as the line between criminal activity and the exercise of freedom of speech is non-existent in China. The development of this new all-encompassing architecture of electronic surveillance will make the lives of such courageous activists even more difficult.

In November 2000, 300 companies from over 16 countries attended a trade show in Beijing called Security China 2000. Among the organizers was the "Chinese Communist Party Central Committee Commission for the Comprehensive Management of Social Security." A central feature of the show was the Golden Shield project, launched to promote "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work." China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to records on every citizen in China, while linking to vast networks of cameras designed to increase police efficiency.

In order to make the Golden Shield a reality, the Chinese government is dependent upon the technological expertise and investment of Western companies. Canada's Nortel Networks is playing a key role in these developments as witnessed by:

> its joint research with Tsinghua University on specific forms of speech recognition technology, for the purpose of automated surveillance of telephone conversations;

> its strong and early support for FBI plans to develop a common standard to intercept telephone communications, known as CALEA, in conjunction with technology transfer through its joint venture, Guangdong Nortel (GDNT);

> its close relationship with Datang Telecom, a Chinese firm with substantial interests in the state security market in China;

> the promotion of JungleMUX which allows video surveillance data to be transported from remote cameras back to a centralized surveillance point to the Chinese Ministry of Public Security (MPS);

> the deployment of its "Personal Internet" suite in Shanghai, greatly enhancing the ability of Internet service providers to track the communications of individual users;

> a US$10 million project to build a citywide fibre-optic broadband network in Shanghai (OPTera) enabling central authorities to monitor the interests of subscribers at the "edge" of the network, principally through the Shasta 5000 firewall, in direct conflict with the right to privacy. This technology will also make it more difficult for dissidents to have clandestine communications and facilitate police monitoring of Internet users attempting to access URLs not judged appropriate by the Chinese government;

> the integration of face recognition and voice recognition technology in collaboration with AcSys Biometrics, a subsidiary of Burlington, Ontario-based NEXUS.[2]

Many other Western firms have been involved in the development of a repressive state security apparatus through the following developments:

> a nationwide database containing information on all adult Chinese citizens;

> smart cards for all citizens which can be scanned without the owner's knowledge at a distance of a few metres;

> closed-circuit television to monitor public spaces;

> technology which allows the Public Security Bureau to make instant comparisons of fingerprints;

> development of firewalls in China.

The self-interested high-tech discourse promises that new information and telecommunication technologies are inherently democratic and will foster openness wherever they are used. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* debunks this myth. Technology is embedded in a social context and, in this report, it has been shown to bolster repression in a one-party state in the name of expanding markets and exponential profits.

Introduction

China has long suffered from inadequate telecommunications. Economic growth has demanded modernization of an infrastructure characterized by outdated technology and limited access to the resources necessary to develop it. To overcome these deficits, the government has embarked on a well-financed effort to modernize its information infrastructure. China has therefore quickly become one of the world's largest consumers of telecommunications equipment.

An important goal of this modernization has been the acquisition of advanced telecommunications equipment from industrialized nations, on the premise that the technologies of the information revolution provide China with the opportunity to "leapfrog" and vastly improve capabilities in areas related to telecommunications. The transfer of these technologies to China has been facilitated by two mutually supporting trends.

First, there is enormous competition among telecommunications firms to get a share of the relatively undeveloped but rapidly expanding Chinese telecommunications market – the largest market in the world. Naturally, the lure of potential billions has attracted every major telecommunications corporation, including US-based Lucent and Cisco, European wireless giants Nokia and Ericsson, and Canada's Nortel Networks – not to mention countless others. From these companies, China is buying more than US$20 billion worth of telecom equipment a year.

China is reported to account for about 25% of the world's market for telecommunications equipment and is expanding exponentially. Much of this growth is achieved through sales by foreign telecommunications companies and by joint ventures with Chinese partners, which brings us to the second important trend.

The installation of an advanced telecommunications infrastructure to facilitate economic reform greatly complicates the state's internal security goals. As the amount of information traveling over China's networks increases exponentially, the government's ability to control that information declines.

The exponential growth of the Internet in China has led some to argue that as new technologies are adopted they will inevitably create a more open, democratic society. The premise of much research is that the Internet is an inherently democratizing medium, promoting pluralism, strengthening civil society, and pressuring governments to become more accountable to their people. In the post-Cold War world, the power of information and communication technology to transform repressive societies is often held to be self-evident.

Recent events in China present a rather different story. It is well documented that the Chinese government is committed to controlling online content and to restricting the access citizens have to information published outside the country.[3] They also aim to prevent the emergence of "virtual organizing" that has become an important feature of the Internet in other countries. In this regard, the Internet presents a number of unique challenges to the regime. Recent data from a Chinese Academy of Social Sciences (CASS) survey shows that 10% of users admit to regularly using proxy servers to defeat censorship, that most users trust foreign news

sources almost as much as government sources, and that the majority believe that the Internet will have significant social and political effects.[4]

In light of this rapid transformation, Chinese authorities are keen to acquire new technologies that will serve to increase their surveillance capabilities. While the Internet may empower ordinary people, it may also provide the government with a new range of repressive tools to monitor private speech and censor public opinion.

Chinese President Jiang Zemin, left, shakes hands with Frank Carlucci, chairman of Nortel Networks of Canada, in March 2000 in Beijing.

From the first linking of China to the global Internet in 1994, central authorities have consistently sought to control China's Internet connections. Heavily restricting international connectivity was a key principle in China's nascent Internet security strategy. Now, seven years later, international connections for all five of China's major networks[5] still pass through proxy servers at official international "gateways."[6] Filtering and monitoring of network traffic is still focused at this level. Derisively termed "The Great Firewall"[7] by hackers and journalists worldwide, this strategy has enjoyed varying degrees of success. Continued economic modernization, however, has led to exponential growth in the demand for international bandwidth, and the sheer volume of Internet traffic today poses a serious challenge to the strategy of State control at the gateway level.

Originally, there were many reasons for constructing the Chinese network along the lines of this "Great Firewall" model. The gateways would modulate the pace of China's opening up to the world through electronic interaction. The government would decide at what rate to expand the connections and could theoretically shut them down in a social emergency.

The gateways were to serve as the first line of defence against anti-government network intrusions. They would serve as a firewall, restricting the amount of information about internal networks available to foreign intruders. The gateways were designed to prevent Chinese citizens from using the Internet to access forbidden sites and anti-government information from abroad. In theory, State control of the routing tables at the gateway level offered authorities the hope that they could prevent their own people from accessing foreign sites like the Cable News Network (CNN), the British Broadcasting Corporation (BBC), the Tibet Information Network or Human Rights Watch/Asia.

China's Internet regulations and legislation are guided by the principle of "guarded openness" – seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination and the use of the Internet by domestic or foreign groups to coordinate anti-regime activity.

The stakes are high – for the government, as China integrates into the global economy, and for the would-be "cyber-dissident," who ultimately faces the death penalty for illegal use of the Internet.

Box 1:
Paying the Price for Freedom

In January 2001, the official news agency Xinhua announced that anyone involved in "espionage activities" such as "stealing, uncovering, purchasing or disclosing State secrets" using the Web or by other means risks the death penalty, or 10 years to life in prison.

> On January 18, 2000, the dissident Leng Wanbao was interrogated for three hours after circulating a letter from another dissident to people outside China over the Internet. The police reminded Leng Wanbao that sending such a letter was against the country's public security laws.

Lin Hai, a computer entrepreneur, was charged with subversion in 1998 for supplying Chinese e-mail addresses to a pro-democracy Internet magazine.

> On March 3, 2000, Lin Hai, a software entrepeneur, who had been condemned to two years in prison for "inciting others to overthrow the State," was freed from prison. Arrested in 1998, he had been convicted of supplying 30,000 Chinese e-mail addresses to overseas dissident publications, notably *VIP Reference*. These publications had used the addresses to distribute dissenting articles over the Internet. Freed in the greatest secrecy in September 1999, Lin Hai was very hesitant to speak of his situation, suggesting that the authorities had offered him early release in exchange for his silence. At his release, Lin Hai called himself "the first Chinese Internet prisoner."

> On June 3, 2000, Huang Qi, manager of www.6-4tianwang.com, which contains a discussion forum, was arrested and accused of "subversion." The authorities accused him of publishing articles on his Web site, which is hosted in the US, condemning the Tiananmen massacre in June 1989. It contained an open letter from the mother of a young student killed during the massacre, calling for the renewal of the 1989 pro-democratic movement.Huang Qi's computer and all of the documents found in his office and home were confiscated. The site, open to "all those who have something to say," is still updated by Chinese dissidents who live in the US, but mainland Internet users can no longer access it.

> On August 16, 2000, the police interrogated Jiang Shihua, a professor of computer science in the Sichuan province in southwestern China. He was accused of "inciting subversion." He used the cybercafé that he owned, the Silicon Valley Internet Coffee, in Nanchong, to circulate articles criticizing the authorities, and published pro-democracy articles in an Internet newsgroup. He has been charged with "inciting others to overthrow the State." This case has still not gone to trial.

> Qi Yanchen, editor of the online publication *Consultations,* was convicted on September 19, 2000, to four years in prison for "subversion" and "circulation of anti-governmental information over the Internet." The MPS claims that he used the pseudonym Ji Li to write articles for the Hong Kong monthly *Kaifang* and the dissident newsletter *VIP Reference.* He also published excerpts of his book, *The Fall of China,* advocating political reform. The police confiscated his computer, his fax and his notes.

> On May 13, 2000, the government suspended the China Finance Information Network site for two weeks and ordered its owners to pay a fine. The online financial publication was accused of having circulated rumours that could damage the image of the government.This conviction followed the publication of an article on corruption concerning a local political official.

> On August 3, 2000, security officials disconnected and banned www.xinwenming.net for having circulated "counter-revolutionary information" and attracting a "large part of the Chinese dissident community." The five dissidents behind the site are currently wanted by the police, but have not yet been arrested. Created April 29, 2000, www.xinwenming.net is the first site hosted in China to openly call for "national reconciliation and democracy."

Technology Transfer and Policy Convergence

The Right to Freedom of Opinion, Expression and Information

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The Universal Declaration of Human Rights, Article 19

Globalization erodes national control of the flow of data. The development of the Internet is perhaps the best known example of a global technology. The combination of globalization and digital convergence is having a devastating effect on privacy in many developing countries. In the field of information and communication technology, the speed of policy convergence is accelerating to such an extent that even the most developed nations can hardly keep up with advances in technology. Across the digital surveillance spectrum – wiretapping, personal ID systems, data mining, censorship or encryption controls – it is the industrialized countries that invariably set the rules for the rest of the world.

There is increasing concern that much of this surveillance technology is being exported, without any end-use criteria, to countries that flagrantly abuse the fundamental human rights of their citizens. Governments of countries with poorly developed infrastructures rely on industrialized countries to supply them with surveillance equipment. The transfer of surveillance technology from the developed to the developing world is now an important component of the post-Cold War arms industry.[8] With scant attention given to differing levels of human rights compliance, standardization across national borders is leading many to argue that a global architecture of electronic surveillance is emerging, with its origins in the US law enforcement community.

Operation Root Canal

As early as 1988, in a program known internally to the US Federal Bureau of Investigation (FBI) as "Operation Root Canal,"[9] US law enforcement officials demanded that telephone companies alter their equipment to facilitate the interception of messages. All but one of the major global telecom companies refused to contemplate altering their equipment. The exception was a Canadian company, Nortel Networks, which agreed to work closely with the FBI.[10] More than 75% of North American Internet backbone traffic travels across Nortel Networks systems, and the company derives a significant proportion of its sales revenue from the US telecom market.

After several years of lobbying by the FBI, the US Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[11] CALEA requires that terrestrial carriers, cellular phone services and other telecom equipment manufacturers ensure that all their "equipment, facilities or services" are capable of "expeditiously... enabling the government... to intercept... all wire and oral communications carried by the carrier... concurrently with their transmission."[12] Communications must be in such a form that they can be transmitted to a remote government facility.

CALEA redefines the telecommunications industry's obligation to assist law enforcement in executing lawfully authorized electronic surveillance. The law directs the telecommunications industry to actively develop solutions to address law enforcement's surveillance requirements. To facilitate compliance, CALEA authorized US$500 million to be appropriated for the purpose of reimbursing the telecommunications industry for certain costs.[13] Manufacturers must work with industry and law enforcement officials to ensure that their equipment meets federal standards. A court can fine a company US$10,000 per day for each product that does not comply.[14]

The passage of CALEA was controversial, not least because the FBI continuously sought to include more and more rigorous regulations under the law. These included requirements that cellular phones allow for location-tracking on demand and that telephone companies provide capacity for up to 50,000 simultaneous wiretaps.[15]

While the FBI lobbied Congress and pressured US companies into accepting CALEA, it also pressured US allies to adopt it as an international standard. The FBI began working with the Justice and Interior Ministers of the European Union (EU) towards creating international technical standards for wiretapping.[16] In 1991, the FBI held a series of secret meetings with EU member states to persuade them to incorporate CALEA into European law. In 1993, the FBI began hosting meetings at its research facility in Quantico, Virginia called "International Law Enforcement Telecommunications Seminars" (ILETS). The meetings included representatives from Canada, Hong Kong, Australia and the EU. At these meetings, an international technical standard for surveillance, based on the FBI's CALEA demands, was adopted as the "International Requirements for Interception."[17]

The plan, according to an EU report,[18] was to call for the industrialized world to agree to norms and procedures and then sell their products to developing countries. Even if they did not agree to interception orders, they would find their telecommunications monitored by the UK-USA signals intelligence network "the minute they used the equipment."[19] The FBI's efforts resulted in an EU Council of Ministers resolution that was quietly adopted in January 1995. The resolution's text was almost word for word identical to the FBI's domestic requirements.[20] The resolution was not formally debated, and was not made public until late 1996.

The ILETS group continued to meet. A number of committees were formed and developed a more detailed standard, which extended the scope of the interception standards. The new standards were designed to apply to a wide range of communication technologies, including the Internet and satellite communications. It also set more detailed criteria for surveillance across all technologies. The result was a 42-page document called ENFOPOL 98 (the EU designation for documents created by the EU Police Cooperation Working Group).[21] In 1998, the document entered the public domain and generated considerable criticism. The committees responded by removing most of the controversial details and producing a new document, called ENFOPOL 19, expanding the type of surveillance to include "IP address, credit card number and e-mail address."[22] In April 1999, the Council proposed the new draft council resolution to adopt the ENFOPOL 19 standards into law in the EU.

In May 1999, the European Parliament approved the ENFOPOL 19 resolution. The vote was taken late on a Friday evening with only 20% of the delegates present, and was subsequently reversed by the Council of Ministers. The rejection has not stopped the European Telecommunications Standards Institute (ETSI) from continuing its work on developing international wiretapping standards.

What do You Want the Internet to Be?

"A human touch. I want it to know who I am."[23]

At a trade show held in Beijing in November 2000, the biggest names in Web technology – "companies that proudly attach themselves overseas to the Internet's reputation for anarchy"[24] – peddled their wares to China's secret police and security officials. Billed as the "largest national security exhibition," Security China 2000 was the second such event sponsored by the Ministry of Public Security (MPS) in as many years. Among the organizers listed was the "Chinese Communist Party Central Committee's Commission for the Comprehensive Management of Social Security,"[25] a body which is in overall charge of the state security apparatus, from controls over migrant workers, to anti-crime campaigns and monitoring dissident activity.

Shanghai Business Magazine recently estimated that the Chinese security industry is enjoying 15% annual growth. Overseas specialists cited in the trade journal *Security World* predict 20% growth for the next three to five years. China is expected to become the second largest security market after the US within 10 years.[26]

The trade show was organized by Hong Kong-based Adsale Exhibition Services Ltd. and drew approximately 300 companies from over 16 countries, as well as 24,500 visitors from over 26 of China's provinces. Special guests included Jia Chunwang, Minister of Public Security. According to Adsale, in comparison to the first Security China exhibit in 1998, in 2000 "the show boasts a 50% increase in international exhibitors and an 80% growth in exhibit space area."[27] Exhibitors included network giants Siemens, Motorola, Cisco Systems, Sun Microsystems, and Nortel Networks. There were participating companies from the US, Israel, France, Germany, the Netherlands, Japan, and Canada, among others. The United Kingdom, world leader in closed-circuit TV, had a special section in the show.

The focus of Security China 2000 quickly became the MPS' new Golden Shield project, launched to promote "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work."[28] China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to registration records on every citizen in China, while linking to vast networks of cameras designed to cut police reaction time to demonstrations.

Though the project is still in its infancy, Chinese industry executives at the trade fair estimated that the government had spent RMB 600 million (US$70 million) on research to date, and that the total spending would likely run many times that.

The Golden Shield project, according to information on the conference Web site, is focused on the following fields of security: "Access Control, Anti-Hacker Intrusion, Communication Security, Computer Accessories & Software, Decryption & Encryption, E-commerce Security, Extranet & Intranet Security, Firewalls, Networking Communications, Network Security & Management, Operation Safety, Smartcard Security, System Security, Virus Detection, IT-related Services and Others."[29]

The success of the Golden Shield project depends on a wide range of advanced technologies. While Chinese research is advancing rapidly in these areas, and other related fields, Chinese scientists have developed none of the components necessary to implement Golden Shield independently. In each case, they have relied on assistance from Western corporations, either by purchasing components as turnkey solutions, or through technology transfer – either through formal business deals or in exchange for greater market access.

The technologies necessary to support an intelligent mass surveillance network are frighteningly complex. However, since the solutions are modeled on human forms of intelligence we can categorize them in terms familiar to everyone: Beijing's Golden Shield surveillance network is intended to be able to "see," to "hear," and to "think."

The technology behind the network's ability to "hear" – to automatically monitor telephone conversations, searching for key words and phrases, for example – centers on speech signal processing. Similarly, video signal processing lies behind a surveillance camera's ability to "see," that is, to recognize individual faces in a crowd of people. Both "senses," forms of digital signal processing (DSP), are termed "algorithmic surveillance" systems, which is data analysis via complex algorithms modeled on the human nervous system. In speech signal processing, for example, the cochlea might be the basis for mathematical abstraction.

In China the leader in each of these fields is the Department of Electronic Engineering at the prestigious Tsinghua University. A research group there has been working on speech recognition since the early 1980s. This research is financially supported by both the Chinese government and Nortel Networks (from 1995 to 1998).[30] It parallels Nortel's own speech recognition research in association with the FBI.

The funds from the Chinese government for the speech recognition project come out of the National 863 High Technology Projects Budgets.[31] The 863 Project was initiated in March 1986 as China's response to the Reagan Administration's Strategic Defense Initiative/"Star Wars."[32] The 863 concentrates government investment in seven distinct areas, including information technology, which have military and state security applications. Other examples of 863 investments include lasers and anti-satellite systems, and some 863 projects are supervised by the Chinese Weapons Development Agency.[33]

By the end of 1998, Tsinghua's engineers announced that they were developing a "large vocabulary speaker independent continuous commands recognition system over telephone channel. This real-time system is used for telephone exchange machine and information service system over telephone connections with the recognition rate over 98%."[34] Future research, they added, will focus on "large vocabulary (if not unlimited) speaker-independent continuous speech recognition, and large vocabulary telephone-based speech recognition… to develop a fast speaker adaptive technology, which can efficiently improve the accuracy of the speaker independent recognition."[35] Such a system parallels the development of the technology required to implement CALEA in the US; in other words it would appear to have no other purpose apart from automated surveillance of telephone communications.

Box 2:

China's Golden Projects:

Modernizing the Chinese Economy

The **Golden Projects** were China's telecommunication and information infrastructure initiatives in the 1990s. The projects were categorized into four phases:

Phase One was comprised of four projects: **Golden Bridge** – the infrastructure for the China National Economic Information Network; **Golden Gate** (Customs) – a foreign trade information network linking the Ministry of Foreign Trade and Economic Cooperation with the Customs Bureau; **Golden Card** – an experimental electronic money project;and **Golden Sea** – an information system linking China's top government leaders and providing them with live access to data from all the institutions, organizations, and offices under the direct jurisdiction of the Communist Party Central Committee.

The projects in Phase Two were designed to apply information networks to economic reform.They comprised: **Golden Macro** – which was the Government's Central Economic and Financial Leading Group for macro-control over national economic activities; **Golden Tax** – a data network designed to link State Tax Administration's auditing centre in Beijing with 50 regional offices and 800 bureaus; and **Golden Intelligence** China's Internet service.

Projects in Phase Three had to do with sectoral applications of the new IT program.They included **Golden Enterprise** – the construction of intranets in China's 12,000 large and medium-sized enterprises, and their interconnection according to different circles of business; **Golden Agriculture** – a databank service network providing agricultural information, weather reports, and market information; **Golden Health** – the Ministry of Public Health's information exchange system for hospitals; **Golden Information** – a network linking the various statistical collection departments across the country; and **Golden Housing** – a nationwide database of information on real estate. Phase Four of projects included **Golden Cellular** – a consortium of China's largest domestic mobile communications manufacturers; and **Golden Switch** – a program to build China's domestic digital switch manufacturing industry.

Unholy Alliance

Tsinghua's engineering faculty has close ties with the Bell-Northern Research Lab (BNR) in Montreal, a Nortel research and development subsidiary,[36] and the laboratory where Nortel's own speech recognition module (STM) was developed. During the Canadian trade mission to China in 1998, Canadian Prime Minister Jean Chrétien announced that Nortel Networks and Tsinghua would establish a joint research laboratory.[37] A primary goal of the research laboratory was to accelerate the development of networking expertise in China. The agreement also included an "expert exchange program" between Nortel Networks and Tsinghua University to facilitate closer collaboration. Indeed, graduates of Tsinghua's engineering department went on to play key roles in developing Nortel's speech recognition module.

Similarly, Tsinghua has "made statistics of the common sentential forms used for telephone calls. Two hundred and fourteen sentential forms of different commands were collected" to develop the world's largest Chinese speech database.[38]

Given Nortel's early involvement in the development of standards in support of the CALEA legislation, it is natural that the first digital switch to reach market, and give service providers and vendors the ability to meet basic CALEA compliance, should be manufactured by Nortel.[39]

The sophisticated DMS Supernode switching technology is manufactured in China through a joint venture with the Chinese government known as GDNT (Guangdong Nortel). At the time, Nortel said of this technology transfer that it "will contribute immeasurably to the development of the Chinese telecommunications industry."[40]

In terms of funding, Nortel invested an extra US$37 million in GDNT (on top of funds agreed in a 1993 Memorandum of Understanding [MOU] with the state planning commission) – an investment that followed hot-on-the-heels of the announcement that the US government would pay equipment manufacturers compensation for the implementation of CALEA.[41]

Beyond the Great Firewall:

from censorship to surveillance

The pace and scale of the development of China's Internet have reduced the significance of the "Great Firewall" strategy of gateways linking to a secure national "intranet." The original China-wide intranet idea was essentially overtaken by events, in particular the liberalization of the Chinese telecommunications sector.

Despite the official policy of openness suggested by China's pending entry into the World Trade Organization, some officials still cling to the dream of a China-only information network sealed off from the dangerous temptations of the World Wide Web.

"China must build a national network that is independent of the Internet," said Jiang Zemin's son, Dr. Jiang Mianheng, a tech-savvy vice president of the Chinese Academy of Sciences, at a conference in Shanghai last June.[42]

The gateway concept, by contrast, has certainly survived, but has been undermined in part by financial and technical factors. The number and speed of the connections have grown to meet increasingly high business and consumer demand, increasing from 84.64 Mbps in the summer of 1998 to more than 351 Mbps at the end of 1999, and to more than 2.5 Gbps by 2001. Concerns for security and control have partially surrendered to economic demands for broadband convergence networks.

The implications of the construction of firewalls to prevent Chinese people from accessing forbidden materials on sites outside the country are well known. Many of the technologies used in these areas of computer security, however, could also be employed to restrict human rights and democracy through intimidation and systematic surveillance of the population.

The MPS announced last year that within three years it would have created a nationwide computerized database containing personal details and ID numbers for every adult in the country. In the past the Chinese government has kept a cumulative file (called the *dangan*) on every individual's performance and attitudes from kindergarten, and throughout adult employment. This information will now be digitized and Chinese citizens will be issued new, second-generation identification cards that will contain their *dangan* on an embedded microchip. Currently, Chinese ID cards consist of a laminated paper card featuring a person's name, photo, birthday and ID number. This paper card "is relatively easy to counterfeit," said Qiu Xuexin, Director of the No. 1 Research Institute under the MPS,[43] speaking recently at the Fourth International Fair of Smart Cards. Qiu added that by using sophisticated encryption it will be more difficult for unauthorized people to access government information in the new card. The second generation smart card is likely to be a "proximity card" – in other words it can be scanned instantly, from several feet away, without the subject necessarily being aware that he or she is being identified.[44]

In addition, last May, the MPS installed on Chinese Internet service providers two "black boxes" – monitoring devices dedicated to tracking the content and activity of individual e-mail accounts. Furthermore, authorities are working with technology experts at Shenzhen University to develop an "e-mail filtration system" that is able to detect and delete "unwanted" e-mails without the recipient's knowledge or consent.[45] Most recently, the MPS has been involved in creating fake proxy servers to conduct surveillance of surfers who try to circumvent official firewalls.[46]

As in 1998, Security China 2000 was held concurrently with its sister event, Building China 2000. The Golden Shield strategy includes plans to construct "intelligent buildings" and a number of vendors promoted their systems at both trade shows. Following the trade shows Chinese-owned Datang Telecom, recently implicated in an industrial espionage case against Lucent, announced that it had won a contract to construct an intelligent building for the Jilin Provincial Public Security Bureau (PSB):

"Under the contract, Datang Telecom will be responsible for the overall design and implementation of this project, accomplishing all tasks including the construction of security monitoring system, integrated wiring, and computer networking. The implementation of this project attaches demonstrative and promotive significance to the Golden Shield that will be started soon in the national public security sector."[47]

Similar plans to integrate CCTV surveillance networks into the urban environment were recently announced by the MPS in Guangdong on a Web site dedicated to promoting the Golden Shield project.[48]

Datang has also developed its own e-mail filtration package and a number of firewalls. Datang enjoys a number of close relationships with overseas telecom manufacturers, including joint research and technology transfer projects. For instance, Datang has benefited from joint research with Nortel when the two collaborated on a project on CDMA wireless protocol, from which Datang developed a Chinese version of the protocol: TD-SCDMA.

While there is considerable evidence that China is conducting its own advanced research and developing homegrown security systems, the IT security field in China remains essentially

dependent on the expertise provided by transnational corporations, through joint venture partnerships, technology transfers, and direct investment – even at the most basic technological level.

Understandably, corporations are not always keen to publicize such a relationship. Motorola, for example, supplies China's traffic police with wireless communication devices. Journalists reported that company representatives at Security China 2000 "refused to answer questions about the firm's involvement in the Golden Shield project…" Orin Li of Compaq China was equally evasive, claiming: "We are not the only company; everybody's doing it. Go and ask Sun!"[49]

Sun Microsystems is indeed involved in transferring high-tech expertise to the Chinese security apparatus. Working with Changchun's Hongda Group, market leaders in fingerprint recognition technology, Sun Microsystems developed a computer network linking all 33 provincial level police bureaus, forming one layer of the Golden Shield, allowing the PSB instant comparison of fingerprints with a nationwide database.

Cisco Systems is another example, having provided a large proportion of the routers and firewalls in China's network. At Security China 2000 a saleswoman for the computer-network giant Cisco Systems told the group of PSB officials that her company was the world leader in firewalls, and that "China is a large potential market for this kind of technology."[50]

Making the Internet Personal

Right to Privacy

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
>
> The Universal Declaration of Human Rights, Article 12

One approach to the problem China's security apparatus faces with the decline in effectiveness of the "Great Firewall" is to shift the focus of content-filtration firewalls from the national level to individual homes and offices – in effect, redistributing the "Great Firewall" from five international gateways to millions of household PCs and cellular phones.

This strategy has profound implications in terms of user privacy – since it makes government surveillance of an individual's traffic a reality, and incorporates technologies that impact heavily on Chinese Internet users right to free expression, making it much more difficult for human rights and democracy activists to communicate with "illegal" information sources, and remain undetected by their government.

This trend, a shift from generalized content control at the gateway level to individual surveillance of users at the edge of the network, is underlined by the advent of new technologies for managing broadband content delivery.

At the Security China 2000 conference Nortel Networks was promoting the JungleMUX digital surveillance network and its OPTera Metro portfolio to the MPS. JungleMUX is a state-of-the-art system for transporting surveillance video from a network of remote cameras back to a control centre. The OPTera Metro portfolio is the mainstay of Nortel's "Personal Internet" initiative, which is designed to enable Internet service providers to better track individual Internet users and their online activities, and thus heavily criticized recently by privacy advocates in the US.[52]

Nortel's presentation at Security China 2000 must have impressed someone. Shanghai Telecom (ST) recently announced that it had selected Nortel's OPTera product portfolio as a next-generation citywide fibre-optic broadband network. The contract estimated to be worth more than US$10 million means that Nortel will build China's first optical city network including a broadband access system and an ADSL solution for high-speed digital service to approximately 200,000 subscribers. The project is due to be completed in time to support Internet and video conferencing services for international media reporting the APEC Leaders' Meeting to be held in Shanghai in October 2001. Shanghai, powerhouse of the new Chinese economy, will be able to boast one of the most advanced citywide networks in the world.

The OPTera package is at the heart of Nortel's Personal Internet strategy and has allowed Shanghai Telecom to build an advanced parallel optical network supporting streaming media and other time critical transactions. Media streaming is very difficult to achieve over conventional Internet circuits. While Nortel's state-of-the-art fibre-optic links will dramatically increase the bandwidth available to the city, that is not the feature that stands out for anyone looking to increase security in the face of new, increasingly sophisticated threats to China's network security. Important components of the OPTera portfolio and key to the Personal Internet strategy are Nortel's Shasta and Alteon products[53], which will enable Shanghai Telecom to offer customized Web services to businesses and consumers. Nortel's "Personal Internet" strategy is all about personalizing content delivery services with a user-aware, content-aware network. This means that the network is designed to "think," that is to identify individual subscribers when they log on, matching names to IP addresses, and learning over time what content interests the subscriber.

> "Imagine a network that knows who you are, where you are, and can reach you whether you're on your mobile phone or at your desktop. Even better, imagine instead of finding your Web content, it finds you. Sounds personal. Exactly."[51]
>
> **– Nortel Networks, Personal Internet Strategy**

The Shasta 5000 BSN is designed to power the subscriber edge of the network, where "last mile" technologies like high-quality DSL meet the Internet backbone, and where broadband subscribers meet broadband services and content. Shasta is a universal aggregation point where conventional dial-up, DSL, fixed and mobile wireless, ATM/frame relay, and leased line connections all join the Internet. Shasta appeals to ST as a means to increase competitive advantage by becoming a value-added broadband services network. It appeals to Shanghai's Public Security Bureau (PSB), the most advanced of China's online police, because of a number of unique security properties it incorporates.

The Personal Internet strategy is presented to ST, as it is in the West, as a means to derive increased profits from its networks by, for example, offering security services or reselling data

to other companies. This practice of reselling personal data, criticized by many privacy advocates, is explicitly ruled out in Nortel Networks own Privacy Statement. Nevertheless, the

Personal Internet strategy depends on the network's ability to match IP addresses to users' demographic profiles.

Nortel believes that its Personal Internet strategy is the key to the future of the Internet, and has put the Personal Internet at the center of its latest publicity drive. It is remarkable that Nortel can enthusiastically promote business practices to other corporations that it claims to avoid in its own operations.

Nortel's Personal Internet strategy enables Shanghai's PSB to move beyond simply tracking Web hits to targeting specific audiences, and creating demographic profiles in real time. Such intelligent network distribution and delivery has a profound impact on user privacy. "Personal Internet" is a network that always "knows who you are."

Internet users coming onto the network via a range of broadband access technologies such as DSL, wireless and cable have security settings applied to them on a per subscriber basis. With an extraordinary level of packet processing, Shasta is one of the most powerful carrier-class platforms for managing network security. Mass market broadband introduces new security concerns with "always on" Internet connectivity. The Shasta 5000 BSN provides extensive firewall capabilities that are simple to provision, and enable constant monitoring of every individual's traffic flow.

> "Nortel Networks will not sell, rent, or share this information with any other organization."[54]
>
> "Nortel Networks collects IP addresses for system administration and internal tracking. When you visit our site, our servers log the IP addresses only. We do not link IP addresses to anything personally identifiable."[55]
>
> **– Nortel Privacy Strategy, 2000.**

Broadband access contrasts with traditional dial-up access, where subscribers dial in through their Internet service provider (ISP), conduct their business, and then log off. The transitory nature of dial-up access provides a limited window of opportunity to exploit any security holes. Therefore, security incidents with dial-up access are limited and have not been widely reported.

On the other hand, businesses with dedicated access connections (T-1, frame relay) are protected, but the high cost of these dedicated connections has made them less viable for the small and medium business markets and particularly for individuals, community groups and non-governmental organizations. Broadband connections are always on and permanently connected to the Internet. Yet today, most DSL and cable subscribers are connected to the Internet without firewalls and are therefore highly vulnerable. This issue poses a real threat to network security.

To counter this, Nortel's Shasta offers a layer of security positioned between personal firewalls and much more expensive corporate solutions. This security integrates an advanced policy-based state-aware firewall capability, with remote authentication, activity logging, encryption, and content filtering. Shasta's position at the edge of the network enables the service provider to apply security policies across each and every subscriber through one simple interface, rather than allowing subscribers to manage their own security.

The "subscriber edge" is the aggregation point in the service provider's network where the subscriber meets the network. It is the only point in the network where the service provider has complete knowledge, control and visibility of the subscriber and his or her traffic flows. Beyond this point, traffic from multiple subscribers gets aggregated over high-speed connections to backbone or core routers. Once traffic reaches the international gateways it lacks the transparency that affords monitoring agencies visibility into each individual subscriber's traffic flows.

Nortel's security solution reflects this principle: "the only viable point in the network where the service provider can apply any effective form of control over the subscriber's traffic is at the subscriber edge." In other words, while security software is located in the subscriber's own PC, it is managed remotely by his ISP. This strategy signals the end of the failed "Great Firewall," in that the focus of surveillance and content control is now on traffic at the edge of the network, rather than the centre – the international gateways.

Another significant feature of Shasta's security is its sophisticated anti-spoofing technology. Spoof attacks involve sending traffic that appears to originate from a legitimate source IP address and is therefore acceptable to the firewall, but the source address has been hijacked and used illegitimately. Even the most advanced firewalls can be and have been spoofed by the serious hacker. The Shasta 5000 BSN can prevent spoof attacks from getting through to the subscriber's network as it incorporates advanced anti-spoofing capabilities that can be applied to each individual subscriber. The Shasta 5000 BSN firewall filters traffic going to and from the subscriber, and prohibits the end-user from generating spoofed packets and from forwarding other subscribers' traffic.

This impacts on a number of areas. While it offers improved defences against distributed denial-of-service attacks, it also presents a challenge to systems that have been created to assist those trying to circumvent China's firewalls. This includes dissidents and democracy activists.

Service providers use identity verification in order to validate users requesting access to their networks. The authentication mechanisms will take many forms. Authentication mechanisms include, but are not limited to, user name and password, smart cards, and biometric devices such as fingerprint scanners or face recognition systems.

The Shasta 5000 BSN supports several forms of user authentication, dependent upon the access mechanism and protocol. For administrator access to the Shasta 5000 BSN, authentication is currently password-based but is designed to be compatible with biometric authentication in the future.

Activity logging helps track activities within and at the edge of a network to determine if rejected traffic represents a threat or forms a pattern. Such information can later be used to enhance the security features of the network and track specified "illegitimate" users.

The Shasta 5000 BSN provides an easy-to-use graphic user interface (GUI) for the creation and definition of full activity logging. With this service, the Shasta provides a log manager that displays every logged event per individual subscriber and per service. The log information is stored and delivered to remote databases. All events, including acceptance and rejection of packets, can be recorded in a log based on actions specified within the system and are time-stamped at the moment they are generated. All packets that are dropped due to non-conformance of a protocol's "normal" behaviour can also be logged in the log manager for later analysis.

Shasta's log manager enables the analysis, filtering and searching of the log in a variety of different ways, so that very detailed information about an individual's communication habits can be extracted quickly and efficiently. This information can then be stored in huge local and centralized databases for subsequent analysis by the MPS. In this way, for example, the MPS can match "real world" events to patterns within Internet traffic. An unusual surge in the number of e-mails sent the day before a demonstration, for example, would yield a lot of intelligence without even accessing the content of the messages.

Content filtering is another way to control incoming Internet content into any environment – home, school, cybercafé and business. Such filtering is done through predetermined filters used to block URLs meeting certain predefined criteria or categories for the particular environment or circumstance. Regional centres for Internet security under the control of the MPS, dedicated to maintaining such URL lists, are springing up throughout China to facilitate the government's information control strategy at a more local level.

Filtering is administered through a proxy in which an individual's Web requests are sent to a proxy server which checks requests against a list of "denied" URLs and blocks any incoming content from those URLs not meeting the Chinese government's predetermined criteria for "wholesome" Web content. The Shasta 5000 BSN has the ability to support just such proxy services through its redirection capability to such content filtering server sites. Through the Shasta 5000 BSN policy-forwarding capability, rules can be established to forward the subscriber traffic to content filtering servers, which then do the filtering on behalf of the government.

Locating content control at a more local level has two important consequences for anyone within China attempting to access information on the MPS' list of forbidden URLs. First it will become significantly more difficult to access such proscribed Web sites in the first place as

Shasta's firewalling capabilities are so much more sophisticated being located at the point where the user joins the Internet. For example, the practice of using proxy servers situated outside of China, currently prevalent among dissidents as a means of circumventing firewalls at the gateway level, will be much easier to detect and log – generating a pattern of use that will, over time, appear suspicious to the network.

Secondly, by assigning responsibility at a regional level for content filtration management, local MPS bureaus will be much more involved in the process of leveraging surveillance data from high-tech sources, and applying it to more low-tech scenarios – integrating Internet data with traditional modes of MPS surveillance, like networks of informers. This process is unmanageable at a centralized level except for the most high-profile cases, but becomes a potent means of control when distributed to regions, cities, and local neighbourhoods.

A Network That Knows Who and Where You Are

Right to Association

Everyone has the right to freedom of peaceful assembly and association.

The Universal Declaration of Human Rights, Article 20

One of the stated objectives of the Golden Shield project is the establishment of a nationwide network of closed-circuit television or CCTV cameras in public spaces to improve police response times to outbreaks of social unrest.[57] The incredible range of surveillance cameras on display at Security China 2000 indicates the extent to which technology is more complex today than years ago. New circuits allow the camera to ignore bright, light-emitting objects within its fields of view; miniaturization allows easier concealment; infrared cameras allow surveillance in darkness.

"The China CCTV market is worth US$350 to US$400 million per year," estimated Gerrit Hurenkamp, Development Manager for the US-based Pelco International. "It's a good market but difficult to get into. They are well educated here and know what they want. You can't just dump any product."

As video surveillance electronics become increasingly sophisticated ever-greater bandwidth is required to transport the stream of images produced from remote locations to control rooms. Such a system requires advanced network architecture, capable of spanning a country as large as China, and Nortel's presentation of its JungleMUX system at Security China 2000 spoke directly to that need. Closed-circuit video signals in Nortel's JungleMUX network are transported over a wide area network (WAN) operating between 1.6 to 44 Mbps and accessible by all the nodes in the network. Each video source (camera, VCR, etc.) is digitized using a user-configurable compression algorithm. This provides an efficient and scalable CCTV transport solution.

Recording can be in several modes: real-time, of varying qualities, and time-lapse. Real-time is like regular TV (at 30 frames per second, showing full motion). Time-lapse selects only a few frames per time period to record. The main advantage of time-lapse is that it allows one tape

Box 3:

"Neutral" Technology at Tiananmen Square

Following the Tiananmen Square massacre in 1989, the Chinese authorities tortured and interrogated thousands of people in an attempt to identify the demonstration's organizers. But even if the students and workers had resisted the terrors of the secret police, the hapless demonstrators stood little chance of anonymity. Stationed throughout Tiananmen Square is a network of UK manufactured surveillance cameras, designed to monitor traffic flows and regulate congestion. These cameras recorded everything that transpired in the months leading up to the tanks rolling into the square.

In the days that followed, these images were repeatedly broadcast over Chinese state television.Virtually all the transgressors were identified in this way. Siemens Plessey, which manufactured and exported the cameras, and the World Bank, who paid for their installation, claim they never had any idea that their "technologically neutral" equipment would be used in this way. However, in 1995 the World Bank authorized the funds to set up the same traffic flow system in Lhasa, the capital of the Tibet Autonomous Region. Lhasa is not, as yet, known for having problems with traffic congestion; besides, the area in which the traffic flow system is in operation is solely for pedestrians.[56]

to record for a much longer time than real-time recording, a particularly useful feature for archival purposes: high-resolution 700x480 colour pictures at 2 frames/sec, using about 400 kbps per camera. The flexibility in bandwidth allocation of JungleMUX Video Mapper allows for requesting higher resolution images and more frames per second from a specific camera, at any given time (up to broadcast-quality 700x480, 30 frames/sec NTSC colour signals, using about 6 Mbps [MPEG-2 quality]). The system even allows for ambient audio channels for public surveillance applications.

The revolution in urban surveillance will reach another level of control altogether – once reliable face recognition software becomes the norm. It will initially be introduced at stationary locations, like turnstiles, customs points, security gateways, etc., to enable a standard full-face recognition to take place. We are at the beginning of a revolution in "algorithmic surveillance" – effectively applying artificial intelligence routines to data analysis via complex algorithms, which enable automatic recognition and tracking. Such automation not only widens the surveillance net, it narrows the mesh.[58]

One company at the forefront of this revolution is AcSys Biometrics Corp., a joint venture between AND Corporation, inventor and developer of Holographic/Quantum Neural Technology, HNeT, and NEXUS, a diversified holding company. NEXUS is a Burlington, Ontario-based company operating through a highly diversified web of autonomous subsidiaries and partnerships.[59] AcSys is a provider of one of the most advanced facial recognition systems on the market. AcSys' Face Recognition System (FRS) is being incorporated into Nortel's own product portfolio. AcSys' FRS approach to security applies a proprietary technology for quick and reliable determination of human identity. It provides a scalable solution that integrates easily with existing systems and applications using standard network protocols.

In relation to Nortel's Personal Internet strategy, Rick Collins, Senior Manager of Nortel's "ProtoNet Project (Disruptive Solutions Implementation)," said of AcSys' FRS:

"Layering AcSys' face recognition's capabilities within Nortel Networks' solutions will make communication networks more personal. In the future, people may be recognized at a location, instead of logging in for some mobility services. I envision a network that knows who you are, and when you tell it, where you are, and can reach you whether you're on your mobile phone or at your desktop."[60]

AcSys Biometrics face and speech recognition system is based on a patented core of artificial intelligence called Holographic/Quantum Neural Technology (HNeT).

HNeT neural networks could power a range of Nortel's applications in the financial, manufacturing, security, surveillance, and medical sectors. With technologies like HNeT, with rates of learning up to 200 times faster than conventional neural nets, facial recognition via CCTV becomes a reality and countries with national CCTV infrastructures will view such technology as a natural extension of their networks. As with the example of the traffic control systems installed in Tiananmen Square and Lhasa, this process of extending a system's surveillance capabilities is one of subtle erosion of rights. The dynamics of this process: continuously upgrading technology and incorporating functions unintended by the design.

Diagram 1:

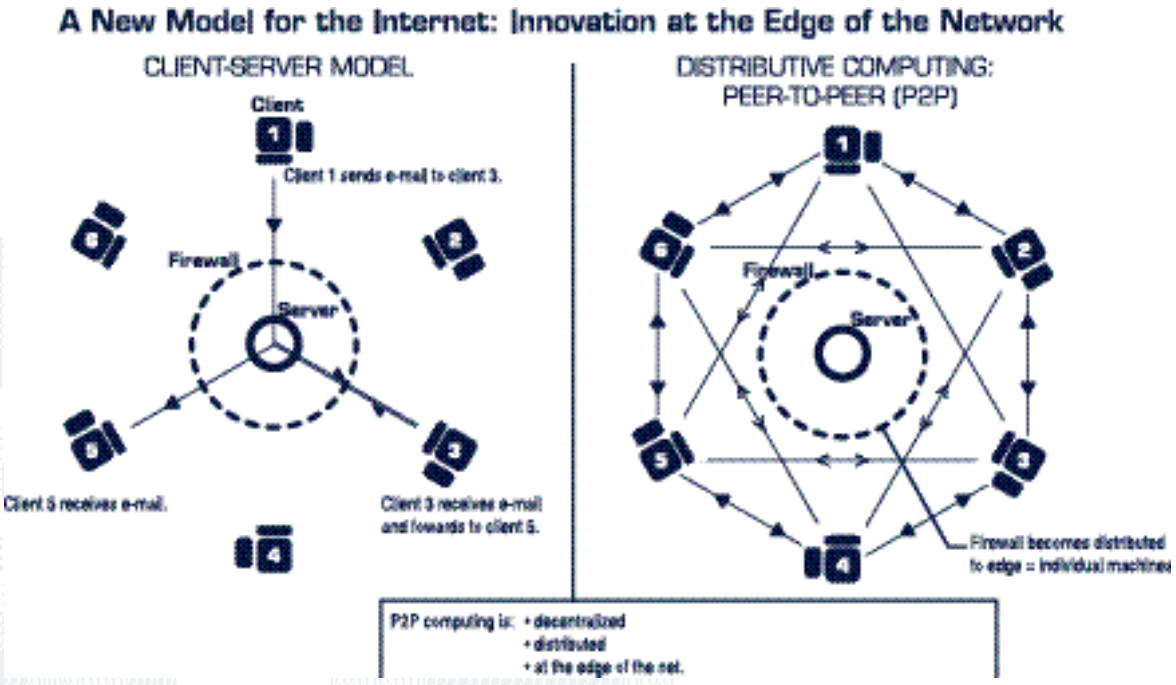
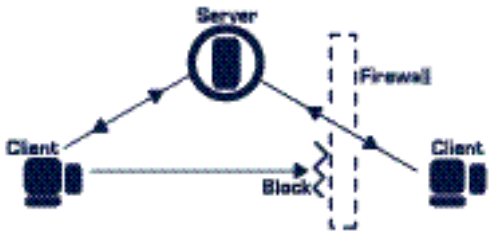

A New Model for the Internet: Innovation at the Edge of the Network
CLIENT-SERVER MODEL
Client
Client 1 sends e-mail to client 3.
Firewall
Server
Client 5 receives e-mail.
Client 3 receives e-mail and forwards to client 5.
DISTRIBUTIVE COMPUTING: PEER-TO-PEER (P2P)
Firewall
Server
Firewall becomes distributed to edge = individual machines
P2P computing is: • decentralized
• distributed
• at the edge of the net.

Diagram 2:


Interaction Across a Firewall
P2P software uses direct P2P communication by default. When a firewall makes direct interaction impossible, most P2P applications automatically send traffic to centralized relay service, where it is packaged as HTTP and "tunneled" through port 80.
Server
Firewall
Client
Client
Block

Conclusion
"The mouse is mightier than the missile"

Democratic accountability is the only criterion that distinguishes Nortel's Personal Internet strategy, voice recognition research, or CCTV transport technology from advanced instruments of repression. In China, the concepts of "state security" and "state secrets," which are the foundation of regulations restricting Internet content and imposing obligations on service providers to monitor users, have routinely been used to punish free speech, block independent organizing and suppress information. In China, there are no privacy rights and government is not accountable through any legal process for the use of information obtained by its security apparatus via surveillance, wiretapping or online monitoring of electronic communication.

In China, as in every country around the world, human rights activists find themselves on the frontline of a new struggle to ensure that technological innovation works in favour of freedom and democracy and not for more and more subtle and sophisticated forms of repression. Many of the companies exhibiting their wares at the Security China 2000 Fair claim to share this objective, promoting their activities as "improving the quality of people's work and lives" (Philips) and "connecting anyone, anywhere, anytime… to the resources they need" (Sun Microsystems).

In practice, however, respect for fundamental human rights is required before such rhetoric rings of more than mere public relations spin. While the proponents of economic globalization flaunt the terminology of "level playing fields" and "rules-based systems," millions of people in China live within a system of political control that affects every aspect of their daily lives. There is no level playing field without freedom. There is no "rules-based system" when rules govern only the commercial dimension of human interaction. There is no freedom when the State routinely violates fundamental human rights.

Democratic governments, including the Government of Canada, must prioritize the promotion of human rights in all aspects of their international relations, including trade and investment. In its 1995 foreign policy statement *Canada and the World*, the Government of Canada affirms this commitment: "… we will make effective use of all of the influence that our economic, trading and development assistance relationships give us to promote respect for human rights."

In 1998 at a conference of non-governmental organizations in Montreal, then Canadian Minister of Foreign Affairs and International Trade Lloyd Axworthy said:

"Technology is changing the equations of power, challenging the conventional channels of communication,distributing and disseminating influence in the broadest possible fashion, to the point of democratizing the channels and getting rid of the gatekeeper… technology has a mind-boggling potential to break through barriers and overcome political obstacles to educate, inform and be an agent of political change… the mouse is mightier than the missile."[61]

Sadly, in China technology is serving no such lofty goals. Multinational companies pioneering the information revolution can no longer argue that their mere presence in China will guarantee increasing respect for human rights. Nor can governments cling to their arguments that open markets will lead automatically to democracy. Instead, in authoritarian and repressive countries where fighting crime is willfully confused with suppressing dissent, a different set of rules must be applied in order to shape political and social development. To ignore this challenge compromises freedom not only in China but in our globalized world, it compromises the freedom of all.

Appendix
How to Use the CD-ROM that Accompanies this Report

Installation:

The following instructions will help you install the CD-ROM for Windows 95/98/ME/2000 and MacOS.

1. Close all open programs on your computer and open your CD-ROM tray.
2. Place the CD-ROM in the tray, graphic side up.
3. When the CD-ROM is placed in the CD-ROM tray and the tray is closed, an autorun feature will launch the installation program.

If you do not have an autorun feature or have it disabled, you may launch the installation program named chinags.exe as follows:

Windows: Double-click the My Computer icon on your desktop. Double-click the icon that corresponds with your CD-ROM drive then double-click the icon labeled chinags.exe.

Mac: Click the CD-ROM icon on the desktop then click the icon labeled chinags.exe.

Liner Notes

> ***In an important sense, the means by which this report is distributed – particularly the Chinese language distribution – is as important as the content of the report itself.***

> **As a consequence of China's Internet legislation – particularly with regards to our obligation to provide access to mainland Chinese readers – and in the course of research and dissemination of this report, a number of open source tools and concepts have been employed. A brief outline of some of them appears below.**

> **If you are attempting to access the online version of this report (located at: go.openflows.org) from within the PRC, please make use of appropriate anti-censorship/anti-surveillance software as provided on the CD-ROM.**

> **On the Web site version and included on the CD-ROM you will find additional material related to the research process including an overview of Chinese legislation and regulations governing electronic communications.**

A Call to Action

At this year's Linux World Conference, Stanford University law professor Lawrence Lessig handed down a challenge to get involved and fight the powers of the "old."[62]

Lessig, famous for his work in cyber law and author of the book *Code and Other Laws of Cyberspace,* described how outdated legislation, big business, government and large corporations have co-opted the "free platform" of the Internet, one that ideally was designed to generate free expression, and instead have created something that stifles innovation.

"What do you want to do about it?" Lessig asked his audience. "I will have no effect stopping this change. The more I talk the less [government and corporations] want to listen, the less they want to hear this story. I'm useless in this battle. The people who can make the difference are you, the people who built this architecture of freedom."

Hacktivismo!

"Hacktivismo and the CULT OF THE DEAD COW are issuing the HACKTIVISMO DECLARATION as a declaration of outrage and a statement of intent. It is our Magna Carta for information rights. People have a right to reasonable access of otherwise lawfully published information. If our leaders aren't prepared to defend the Internet, we are."

"A Special Message of Hope," July 4, 2001[63]

Patrick Ball

"Hacktivism is using technology in the service of human rights," said Dr. Patrick Ball, the deputy director of the American Association for the Advancement of Science Human Rights program who has worked on United Nations human rights projects investigating war crimes and genocide as well as on projects in Guatemala, Haiti and South Africa, among others.

PGP

Many human rights groups use cryptography and encryption software such as PGP (Pretty Good Privacy) to protect their messages and information, which is often a matter of life and death. PGP, in its ability to keep information from falling into the wrong hands and to verify whether messages are authentic through the use of digital signatures, "has had an enormous impact on human rights." [See CD-ROM.]

Rubberhose

(pronounced Marutukku)

Rubberhose was originally conceived by crypto-programmer Julian Assange as a tool for human rights workers and journalists who needed to protect sensitive data in the field, particularly lists of activists and details of incidents of abuse.

The Rubberhose programmers met with human rights groups and heard first-hand accounts of such abuses. Human rights workers often carry vital data on laptops through the most dangerous situations, sometimes being stopped by military patrols who would have no hesitation in torturing a suspect until he or she revealed his or her passphrase to unlock the data.

Freenet

Freenet is a massive P2P network that pools the power of member computers around the world to create an archive open to anyone to freely publish or view information of all kinds. Version 1.0 of this report is published on Freenet in three languages, and is therefore available throughout China and the rest of the world. [See CD-ROM.]

SafeWeb

Internet in China catalyst for social change?

SafeWeb is an SSL-encrypted anonymous proxy service that is currently used approximately 100 million times per month by hundreds of thousands of people worldwide, making it the most popular Web site in the world.

Triangle Boy is an open source program that lets volunteers turn their PCs into gateways into the SafeWeb network, thereby foiling attempts of restrictive governments to censor the Internet. Triangle Boy uses IP spoofing and packet routing technology to minimize the bandwidth consumption on volunteer machines. [See Diagram 2: Interaction Across a Firewall.]

Glossary

ADSL (Asymmetrical Digital Subscriber Line)

ADSL is used for moving data over regular phone lines. An ADSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. The ADSL circuit must be configured to connect two specific locations, similar to a leased line. ADSL allows downloads at speeds of up to 1.544 megabits (not megabytes) per second, and uploads at speeds of 128 kilobits per second.

Asynchronous Transfer Mode (ATM)/Frame Relay

A networking technology that contains a flexible multiplexing and switching technique which provides variable bandwidth for local area and wide area networks. Unlike ordinary synchronous configurations, ATM permits flexible allocation of available bandwidth for data, voice, images and video. ATM uses a scalable architecture, making it easily upgradable; it allows a virtually unlimited number of users to have dedicated, high-speed connections with high-performance network servers. Engineering studies indicated that ATM is theoretically capable of data rates of 622 Mbps over fibre optic and 155 Mbps over conventional copper.

Bandwidth

Literally, the frequency width of a transmission channel. Often used as an expression of the amount of data that can be sent through a circuit. The greater the bandwidth, the greater the amount of data that can travel in a given time period.
How much can you send through a connection? Usually measured in bits per second. A full page of English text is about 16,000 bits. A fast modem can move about 15,000 bits in one second. Full-motion full-screen video would require roughly 10,000,000 bits per second, depending on compression.

"Black Box"

A device Internet service providers fit to their servers that relays a copy of all data sent through the system to the state security service.

Broadband

When the bandwidth of a signal is large, it can simultaneously carry many channels of information. Fibre optic cable, in particular, has very high bandwidth, and is referred to as broadband.

Carrier

A telecommunications company that resells communications services to other businesses.

Carrier-Class

A modifier describing network equipment that has the high standards of reliability levels required to serve Internet service providers (ISPs). Carrier-class equipment usually offers at least 99.999% levels of reliability.

CDMA (Code Division Multiple Access)

A digital mobile wireless access protocol used for voice and data. It is being deployed worldwide and is based on spread spectrum technology. Datang has developed a Chinese version of the protocol: TD-SCDMA.

Compression (Algorithm)

Compression is a technique to make a file or a data stream smaller for faster transmission or to take up less storage space.
An algorithm is a formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clearly defined end point.
One everyday example of an algorithm is a recipe for baking a cake. Inventing elegant algorithms – algorithms that are simple and require the fewest steps possible – is one of the principal challenges in programming.

Convergence

The merging of two or more disparate disciplines or technologies. For example, the "fax revolution" was produced by a convergence of telecommunications technology, optical scanning technology, and printing technology. In a broader sense (New Media) convergence often refers to the merging of broadcast television, the Internet, and the personal computer.

Fibre optic

Light transmission through flexible transmissive fibres for communications

Filtering (Packet)

Controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or stopping them based on the Internet Protocol (IP) addresses of the source and destination. Packet filtering is one technique, among many, for implementing firewalls.

Firewall

A system designed to prevent unauthorized access to or from a private network.Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques:

> **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is highly susceptible to IP spoofing.

> **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

> **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Gateway

Also known as application proxy, an application gateway is an application program that runs on a firewall system sitting between two networks. When a client program establishes a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall.This creates two connections:one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected. While this is considered a highly secure method of firewall protection, application gateways require great memory and processor resources compared to other firewall technologies.

Gbps

Short for gigabits per second, a data transfer speed measurement for high-speed networks such as Gigabit Ethernet. When used to describe data transfer rates, a gigabit equals 1,000,000,000 bits.

“Intelligent Buildings”

Intelligent buildings use electronics extensively to manage

> energy efficiency

> security systems

> telecommunications systems

> workplace automation

The ultimate dream in the design of an intelligent building has always been to integrate the four operating areas into one single computerized system. All the hardware and software would be furnished by a single supplier.

IP

Abbreviation of Internet Protocol. IP specifies the format of packets, sometimes called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time. The current version of IP is IPv4. A new version, called IPv6, is under development.

IP Addresses (Internet Protocol Number)

Sometimes called a dotted quad. A unique number consisting of four parts separated by dots, e.g.163.113.245.2.

Every machine that is on the Internet has a unique IP number – if a machine does not have an IP number, it is not really on the Internet. Most machines also have one or more domain names that are easier to remember.

IP Spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted port. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted port and then modify the packet headers so that it appears that the packets are coming from that port .Newer routers and firewall arrangements can offer protection against IP spoofing.

Intranet, National or "China Wide Web"

A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use. As the Internet has become more popular many of the tools used on the Internet are being used in private networks, for example, many companies have Web servers that are available only to employees.

Mbps

Short for megabits per second, a measure of data transfer speed. Contemporary networks, for example, are generally measured in Mbps, which refers to one million bits per second.

Mux (Multiplexor)

Combines multiple signals (analogue or digital) for transmission over a single line or media. A common type of multiplexing combines several low-speed signals for transmission over a single high-speed connection.

Network

A group of two or more computer systems linked together. There are many types of computer networks, including:

> **local area networks (LANs):** The computers are geographically close together (that is, in the same building).

> **wide area networks (WANs):** The computers are farther apart and are connected by telephone lines or fibre optic.

In addition to these types, the following characteristics are also used to categorize different types of networks:

> **topology:** The geometric arrangement of a computer system. Common topologies include a bus, star, and ring.

> **protocol:** The protocol defines a common set of rules and signals that computers on the network use to communicate. One of the most popular protocols for LANs is called Ethernet. Another popular LAN protocol for PCs is the IBM token-ring network.

> **architecture:** Networks can be broadly classified as using either a peer-to-peer (P2P) or client-server architecture.

Computers on a network are sometimes called nodes. Computers and devices that allocate resources for a network are calledservers.

Peer-to-Peer (P2P)

A type of network in which each computer has equivalent capabilities and responsibilities. This differs significantly from the client-server architecture, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally much simpler, but they usually do not offer the same system performance under heavy bandwidth loads. [See Diagram 1.]

Proxy Servers

A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Routing (Tables)

In internetworking, routing is the process of moving a packet of data from source to destination. Routing is usually performed by a dedicated device called a router. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a routing table to determine the best path.

Smart Card

A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit (IC). Smart cards containing an IC are sometimes called integrated circuit cards (ICCs).

Smart cards are used for a variety of purposes, including:

> Storing a patient's medical records

> Storing digital cash

> Generating network IDs

Spam

Bulk unsolicited e-mail.

Streaming Media

A technique for transferring data such that it can be processed as a steady and continuous stream. Streaming technologies are becoming increasingly important with the growth of the Internet because most users do not have fast enough access to download large multimedia files quickly. With streaming, the client browser or plug-in can start displaying the data before the entire file has been transmitted.

TCP/IP

Transport Control Protocol/Internet Protocol, communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols also support TCP/IP.

Endnotes

[1] HONG KONG IS SWALLOWED UP, by Jeff Jacoby, *The Boston Globe*:http://www.bigeye.com/jj070197.htm
CHINESE CHECKERS, OxBlood Ruffin, CDC
http://www.cultdeadcow.com/cDc_files/cDc-0361.html
The Money Trap, A book review by Robert Kagan
Reprinted by permission of *The New Republic*
Originally published April 7, 1997
http://www.ceip.org/people/kagrep1.htm

[2] See endnote 59

[3] http://www.hrw.org/backgrounder/asia/china-bck-0701.htm. Freedom of Expression and the Internet in China, A Human Rights Watch Backgrounder

[4] Ibid, Dr. Stephen Hsu citing a CASS survey – Dr. Guo Liang, China Academy of Social Sciences, May 2001

[5] (CHINANET, CHINGBN, CERNET, CSTNET, and UNINET)
[See Diagram 1: A New Model for the Internet: Innovation at the Edge of the Network.]

[6] Translation of "churukou xindao"

[7] See, for example, http://www.wirednews.com/wired/5.06/china_pr.html
5.06 - June 1997, The Great Firewall of China, Geremie R. Barme and Sang Ye

[8] Big Brother Incorporated, Privacy International:http://www.privacy.org/pi/reports/

[9] http://www.cpsr.org/alert/cpsr.alert.2.05.html. Volume 2.05, November 12, 1993. Published by
Computer Professionals for Social Responsibility
Washington Office
(Alert @ washofc.cpsr.org)
Operation "Root Canal" Documents Released: Questions Raised about FBI's Digital Telephony Initiative
"In response to a CPSR Freedom of Information Act lawsuit, the FBI this week released 185 pages of documents concerning the Bureau's Digital Telephony Initiative, code-named Operation "Root Canal." The newly disclosed material raises serious doubts as to the accuracy of the FBI's claim that advances in telecommunications technology have hampered law enforcement efforts to execute court-authorized wiretaps."

[10] Original source:
http://www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html.
Nortel has subsequently removed this URL from its Web site. However, a copy of the original page remains in Google's Web cache and can be located here: http://www.google.com/search?q=cache:ljjs4pWPJ8Y:www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html
"Nortel has been actively involved in ad hoc committees established prior to the law being enacted. We have been active participants during the standards process with technical representatives at key meetings."

[11] Final version (Enrolled Bill) as passed by both Houses:
http://thomas.loc.gov/cgi-bin/query/z?c103:H.R.4922.ENR:H.R.4922
To amend title 18, US Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other...

[12] Ibid, text from CALEA act

[13] http://www.askcalea.net/about/doj990914.htm
Department of Justice and FBI Reach First Agreement Under Communications Assistance for Law Enforcement Act

[14] http://www.askcalea.com/about/pl103414.htm
"(1) IN GENERAL – A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify."

[15] http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/1997013101.html
1997 B.C. Intell.Prop. & Tech. F. 013101
Government Tempers Electronic Surveillance Proposal; Critics Laud Changes But Are Not Satisfied
by Adam White Scoville, Staff Writer
See also: http://www.cdt.org/publications/pp_3.01.html
CDT POLICY POST Volume 3, Number 1, January 17, 1997

[16] See ENFOPOL timeline: http://www.heise.de/tp/english/special/enfo/6382/1.html.
See also: EU Document 496Y1104(01)
http://europa.eu.int/eur-lex/en/lif/dat/1996/en_496Y1104_01.html
"Whereas in accordance with a decision by the Trevi Ministers in December 1991 a study should be made of the effects of legal, technical and market developments within the telecommunications sector on the different interception possibilities and of what action should be taken to counter the problems that have become apparent..."

[17] The full text of all ENFOPOL documents cited in this paper can be found at http://www.statewatch.org/eufbi/index.html.
At the first meeting of the new Council of Justice and Home Affairs Ministers in Brussels on November 29 and 30, 1993, they adopted the following Resolution on "the interception of telecommunications" which speaks for itself, and is reproduced here in full:
"COUNCIL RESOLUTION ON THE INTERCEPTION OF TELECOMMUNICATIONS
The Council:
1. calls upon the expert group to compare the requirements of the Member States of the Union with those of the FBI;
2. agrees that the requirements of the Member States of the Union will be conveyed to the third countries which attended the FBI meeting in Quantico and were mentioned in the memorandum approved by the Ministers at their meeting in Copenhagen (Sweden, Norway, Finland [countries applying for accession to the European Community], the USA and Canada) in order to avoid a discussion based solely on the requirements of the FBI;
3. approves for practical reasons the extension to Hong Kong, Australia and New Zealand (which attended the FBI seminar) of the decision on co-operation with third countries which was taken at the Ministerial meeting in Copenhagen;
4. hereby decides that informal talks with the above-named countries may be envisaged: to that end the Presidency and the expert group might, for example, organize a meeting with those third countries to exchange information."

[18] See www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf:
SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA
DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE
OF ECONOMIC INFORMATION
Vol.5/5: The perception of economic risks arising from the potential vulnerability of
electronic commercial media to interception

[19] http://www.oneworld.org/index_oc/issue198/codewar.html: The code war
David Banisar & Simon Davies. David Banisar is an attorney at the Electronic Privacy Information Center (EPIC) in Washington, DC and deputy director of Privacy International (PI). He is coauthor of a new book on encryption policy: *The Electronic Privacy Papers: The Battle for Privacy in the Age of Surveillance*. Simon Davies is director general of PI, the author of *Big Brother* and a visiting fellow at the London School of Economics.

[20] www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf

[21] http://www.statewatch.org/eufbi/index.html

[22] Draft COUNCIL RESOLUTION on the lawful interception of telecommunications in relation to new technologies ENFOPOL 19, March 15, 1999: http://www.fipr.org/polarch/enfopol19.html

[23] What do you want the Internet to be? http://www.nortelnetworks.com/corporate/internet/what_do_you_want/index.html

[24] China looks for new technology to police Net
By Martin Fackler, Associated Press, November 9, 2000

[25] http://www.adsaleexh.com/sec/press2.html
Press Release, August 29, 2000
Over 300 International Exhibitors Gather in Security China 2000
Taping the Lucrative China Market

[26] Ibid

[27] http://www.adsaleexh.com/sec/press1.htmmime text/html
Press Release, March 10, 2000
The No. 1 International Security Exhibition back to Beijing again

[28] Ibid, Adsale

[29] Ibid, Adsale

[30] Research Overview, Speech Signal Processing and Intelligence Technology Group Department of Electronic Engineering, Tsinghua University
http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm
Tsinghua has subsequently removed this URL from its Web site. However, a copy of the original page remains in Google's Web cache and can be located here:
http://www.google.com/search?q=cache:4EwAlksjbU:www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm+863+tsinghua+engineering+speech+continuous&hl=en

[31] Ibid

[32] http://www.most.gov.cn/English/Programs/863/menu.htm

[33] http://138.110.28.9/acad/intrel/chinmc.htm
EVAN A. FEIGENBAUM, "China's Military-Civilian Complex," *New York Times*, May 22, 1998

[34] Ibid, 27

[35] Ibid

[36] BNR operates and supports research laboratories at many sites around the world, including two in Canada (Ottawa and Montreal), three in the US (Raleigh, Richardson, and Atlanta), four in the United Kingdom (Harlow, New Southgate, Maidenhead, and Monkstown), one in Japan (Tokyo), one in Australia (Sydney), and one in China (Beijing).

[37] Nortel Networks Signs Contracts Valued At Over US$120 Million During Canadian Prime Minister Jean Chrétien's Visit to China
http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[38] http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm

[39] Specific compliance targets – known as J-STD-025 – establish standards for basic CALEA compliance: see Nortel's DMS-500 Series Platform, Document no: 51047-16-12-00.pdf.

[40] http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[41] Over US$100 million in the case of Nortel according to the US Dept. of Justice: see www.doj.gov.

[42] http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[43] According to a June 12 report in *China Daily*.

[44] http://www.smartcards-china.com/en/page_ehydt1.htm

[45] http://www.state.gov/www/global/human_rights/1999_hrp_report/china.html.Archive site for State Department information prior to January 20, 2001.
1999 Country Reports on Human Rights Practices
Released by the Bureau of Democracy, Human Rights, and Labor
U.S. Department of State, February 25, 2000

[46] Reported in Mingbao, courtesy of Judy Chen, HRIC

[47] http://www.telecomn.com/english/china_comm/CN_200010.htm. DATANG TELECOM CONTRACTS "INTELLIGENT BUILDING WEAK CURRENT ENGINEERING" FOR JILIN PROVINCIAL PUBLIC SECURITY DEPARTMENT

[48] http://www.gzjd.gov.cn/gzjd/

[49] Ibid, AP

[50] China online, http://www.chinaonline.com/topstories/001114/1/c00111456.asp

[51] http://www.nortelnetworks.com/corporate/leadership/personal/

[52] "The idea that ISPs are watching where [customers] go is unacceptable… it's like the Post Office looking into your mail in order to decide what kind of junk to send you." (Junkbusters.org) Several privacy bills are currently being introduced or reintroduced into the US Congress and state legislatures across the US. One bill being reconsidered by Congress, the Spyware Control and Privacy Protection Act, tries to protect online users from software like Nortel's Personal Internet technology. Of course, in China, spam and telemarketing are the least of Internet users worries.

[53] In addition to OPTera Metro, Nortel Networks solution for Shanghai Telecom includes Nortel Networks Shasta* 5000 Broadband Service Node (BSN) and Nortel Networks Passport* 15000 and Passport 7480 multiservice switches.

[54] http://www.nortelnetworks.com/help/legal/

[55] Ibid

[56] AN APPRAISAL OF THE TECHNOLOGIES OF POLITICAL CONTROL, An Omega Foundation Summary & Options Report For the European Parliament, September 1998

[57] Ibid 22 (AP)

[58] (See Norris, C., et. al, 1998.)

[59] Nexus (www.nxsgrp.com and www.nxs.ca), known formerly as Heritage Concepts International (HCI). NEXUS Group International Inc. AND Corporation (www.andcorporation.com). AcSys Biometrics Corp. (www.acsysbiometricscorp.com).

[60] http://www.andcorporation.com/press/press_3_12_01.html. AcSys Biometrics Accompanies Nortel Networks to CeBIT 2001.

[61] Bob Paquin, *The Ottawa Citizen*. Web posted Monday October 26, 1998, E-Guerrillas in the mist.

[62] Linux World Conference:http://www.linuxworld.com/

[63] http://www.cultdeadcow.com/cDc_files/declaration.html

"If you always stand straight,
then your shadow can never be crooked."
> Liu Qing, former political prisoner

Other Publications by Rights & Democracy:
(Visit our Web site at www.ichrdd.ca for a complete list of publications.)
A Human Rights Framework for Trade in the Americas, by Diana Bronson and Lucie Lamarche, 2001.
The Bilateral Human Rights Dialogue with China: Undermining the International Human Rights Regime, 2001.
Protecting Human Rights in a Global Economy: Challenges for the World Trade Organization,
by Robert Howse and Makau Mutua, 2000.
Canadian Mining Interests and Human Rights in Africa in the Context of Globalization, by Bonnie Campbell, 1999.
Women and Peacebuilding, by Dyan Mazurana and Susan McKay, 1999.
Putting Conscience into Commerce: Strategies for Making Human Rights Business as Usual, Volume 2, by Craig Forcese, 1997.
Human Rights: APEC's Missing Agenda, 1997.

```
<html>
<head>
 <title>Droits et D&eacute;mocratie - Centre international des droits de la personne et du
d&eacute;veloppement d&eacute;mocratique</title>
<base target="contenu"></head><!-- frames -->
<frameset cols="18%,82%">
<frame src="http://www.ichrdd.ca/111/navigationFrancais.html"
      name="chinas golden shield"
      frameborder="0"
    framebordercolor="e4e3ca"
      scrolling="fiuto"
      noresize
      marginwidth="5"
      marginheight="5">

<frame name="contenu" src="http://www.go.openflows.org/111/page1china.html" marginwidth="5"
marginheight="5" scrolling="auto" frameborder="0" framebordercolor="e4e3ca" noresize>
</frameset>

<body link="000000" alink="000000" vlink="000000">



</body>
```

Rights & Democracy

International Centre for Human Rights
and Democratic Development

1001 de Maisonneuve Blvd. East, Suite 1100 > Montréal (Québec) H2L 4P9
Tel.: 1 (514) 283-6073 > Fax: 1 (514) 283-3792 > E-mail: ichrdd@ichrdd.ca > Web site: www.ichrdd.ca